Department of Homeland Security Daily Open Source Infrastructure Report for 29 March 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- IDG News reports that 108,000 Florida state employees are being warned that their personal information may have been compromised after work on the state's People First payroll and human resources system was improperly subcontracted to a company in India. (See item 8)

- The Honolulu Advertiser reports landowners across Hawaii are closely examining the reservoirs and dams they own after the March 14 Kaloko Dam collapse that killed seven people living along the Wailapa Stream. (See item 32)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 28, Reuters* — **Indonesia to keep more natural gas as LNG contracts lapse.** Indonesia, the world's biggest liquefied natural gas (LNG) exporter, said on Tuesday, March 28 it would favor domestic gas sales after major export contracts to Japan lapse at the end of this decade. Indonesia, which has far more gas than it has oil, is trying to phase out costly oil−fired power generation and use more of its cheaper, cleaner natural gas domestically, but faces limited supplies due to long−term LNG export commitments. President Susilo Bambang Yudhoyono said, "(LNG) exports will not be stopped, but the ratio will be reviewed, so most of the gas flows for domestic needs." Indonesia now exports nearly half of its natural gas

production in the form of super−cooled LNG. Customers in Japan, which takes about two−thirds of Indonesia's LNG, have already been searching for alternatives. The reduction would most likely come from Bontang LNG, which ships about 85 percent of Indonesia's LNG. U.S. oil major Chevron is a major supplier of gas to the plant.
Source: http://asia.news.yahoo.com/060328/3/2i3kl.html

2. *March 27, Associated Press* — **TransMontaigne finds buyer.** TransMontaigne Inc. said Monday, March 27, it has sold itself to SemGroup L.P., a company that owns and operates pipelines, terminals, storage tanks, among other energy infrastructure. TransMontaigne, operating in the Mississippi River corridor, owns and operates 43 petroleum terminals with a capacity of about 15 million barrels of oil. The deal is still subject to approval by stockholders and regulatory agencies.
Source: http://biz.yahoo.com/bizj/060327/1264997.html?.v=1

3. *March 27, Bloomberg News* — **Exxon Mobil gains piece of oil field in Abu Dhabi.** Exxon Mobil Corp. has signed a contract with the government of Abu Dhabi to help boost output from the Upper Zakum oil field, the fourth largest in the world. The company will take a 28 percent stake in the field, and boost output by 50 percent to 750,000 barrels a day, Abu Dhabi National said Monday, March 27. Exxon Mobil beat rivals Royal Dutch Shell and BP to develop the field. International companies are competing for limited access to Persian Gulf reserves controlled by state producers.
Source: http://www.chron.com/disp/story.mpl/business/energy/3752275. html

4. *March 27, Reuters* — **U.S. and British hostages freed in Nigeria.** Nigerian militants freed three foreign oil workers on Monday, March 27 after five weeks in captivity and said their fighters would now focus on crippling oil supplies from the world's eighth largest exporter. The kidnapping had tied up hundreds of fighters, the perpetrators said, who would be better used to extend a three−month campaign of sabotage against oil pipelines and platforms that has already cut a quarter off Nigeria's 2.4 million barrels per day output. The rebel Movement for the Emancipation of the Niger Delta (MEND) had demanded as conditions for their freedom more local autonomy over the delta's oil wealth, the release of two jailed Ijaw leaders, and compensation for oil pollution. On Monday they said the release was unconditional. "Care for these hostages tied down close to 800 of our fighters (who) would be put to better use attacking oil facilities," MEND said. The attacks on oil facilities have forced oil companies to cut 630,000 barrels a day of oil production. Royal Dutch Shell, which has been worst hit by the attacks, said it would not resume normal operations until it was safe to do so.
Source: http://news.yahoo.com/s/nm/20060327/ts_nm/nigeria_hostages_d c_10

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *March 28, Washington Post* — **Credit card scam investigated in Washington, DC.** A woman posing as a Washington Post employee is suspected of duping dozens of the newspaper's advertisers into turning over their credit card numbers, according to the Post and the U.S. attorney's office. Using the telephone numbers placed in classified ads, the woman would call advertisers claiming that she worked for the paper, Post spokesperson Eric Grant said on Monday, March 27. The woman would explain that the advertiser's credit card number had not gone through and that she needed to run it again. After the person provided the card information, the woman would use it to start making charges to that account. The inquiry is now in the hands of the U.S. Postal Inspection Service, which is frequently involved in investigating identity theft, and the investigation appears to be coming to a close.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/03/27/AR2006032701368_pf.html

6. *March 27, IDG News Service* — **Two new Websites let users find and report phishing.** Security vendors are launching two Websites aimed at helping people report and avoid phishing attacks. The Phishing Incident Reporting and Termination Squad is a volunteer effort designed to take down phishing sites; CipherTrust's PhishRegistry.org site, scheduled for launch Tuesday, March 28, is a service designed to warn legitimate Websites when they are being spoofed by phishers.
Source: http://www.infoworld.com/article/06/03/27/76850_HNantiphishi ng_1.html

7. *March 27, News 5 Boston (MA)* — **Sensitive information stolen from state staffer.** The Massachusetts Department of Mental Retardation (DMR) confirmed Monday, March 27 that the identities of more than 1,600 clients may be at risk after a staff member had a workbag stolen from his car in Lynn which contained a list of individuals registered with DMR, including names, addresses, birth dates, phone numbers, and social security numbers. DMR sent a letter on Tuesday, March 14 informing parents and guardians of the incident. To date, there have been no reports of fraud.
Source: http://news.yahoo.com/s/wcvb/20060327/lo_wcvb/3358311

8. *March 24, IDG News Service* — **Offshoring cited in Florida data leak.** Florida state employees are being warned that their personal information may have been compromised after work on the state's People First payroll and human resources system was improperly subcontracted to a company in India. Employees who worked for the state during an 18 month period between January 1, 2003 and June 30, 2004 may be affected, according to an e−mail message sent to all state employees on Thursday, March 16. The state's Department of Management Services (DMS), which oversees the People First system, estimates that 108,000 current and former state employees may be affected by the data breach, although that estimate could change as the department's investigation into the matter continues. The e−mail was sent after a subcontractor of outsourcing service provider Convergys improperly allowed subcontractors in India to index state personnel files, said DMS spokesperson Tiffany

Koenigkramer. Convergys says that this offshore work was done without its knowledge. The DMS is investigating the matter, but it has so far detected "no known cases of credit fraud or identity fraud that resulted from this work," Koenigkramer said.
Source: http://www.infoworld.com/article/06/03/24/76798_HNoffshoreleak_1.html?source=rss&url=http://www.infoworld.com/article/06/03/24/76798_HNoffshoreleak_1.html

[Return to top]

Transportation and Border Security Sector

9. *March 28, Associated Press* — **Northwest sues airports commission to rid itself of debt.** Northwest Airlines has sued the Metropolitan Airports Commission in hopes of voiding a $130 million debt. The lawsuit, filed Thursday, March 23, in bankruptcy court in New York, claims that a special facility financing deal for space Northwest uses at Minneapolis−St. Paul International Airport is really a loan, not a lease. Northwest is Michigan's leading passenger air carrier with a hub at Detroit Metropolitan Airport. In a bankruptcy, leaseholders continue to get paid. But according to the lawsuit, if the financing is a loan, "Northwest has no obligations ... with respect to the financing." It also says that bondholders, as unsecured creditors, aren't owed anything except what they might get after a reorganization plan or Chapter 7 liquidation. Northwest filed for Chapter 11 bankruptcy September 14.
Source: http://www.usatoday.com/travel/flights/2006−03−28−northwest− lawsuit_x.htm

10. *March 28, Boston Globe* — **Options offered to fix Boston's Storrow tunnel.** State officials have unveiled four options to fix or replace a half−century−old tunnel on Storrow Drive, raising the curtain on a mammoth construction project that could require at least 18 months and up to four years of major construction on one of Boston's busiest thoroughfares. The department came up with the four options after officials determined that the 55−year−old tunnel, which accommodates more than 100,000 vehicles a day, has a usable life of less than five years. Already, the roof is leaky, the steel beams holding it together have corroded, and chunks of concrete have rained down on the roadway. This year, the tunnel was given a zero rating under Federal Highway Administration criteria judging the lifespan of bridges and underpasses, indicating that it needs to be replaced. A final plan is expected by next summer, and construction could begin later in 2007. "This is a project that has an enormous number of stakeholders, from the Back Bay to commuters throughout Eastern Massachusetts," said Joseph O'Keefe, assistant secretary of the state's Executive Office of Environmental Affairs.
Source: http://www.boston.com/news/local/massachusetts/articles/2006/03/28/4_options_offered_to_fix_storrow_tunnel/

11. *March 28, Macon Telegraph (GA)* — **Plan would privatize airports.** The private company managing Macon, GA's airports under a temporary contract would take over long−term if the city pays the cost of running the airports plus a $15,000 monthly management fee, according to its proposal to privatize the city's aviation department. TBI Airport Management's proposal was the only one turned in by a Friday, March 24, deadline set by the city. It's also unclear how much it would cost to operate the airports under either plan, since recent crackdowns from federal regulators have forced the city to make changes at Middle Georgia Regional Airport to keep it open to commercial flights. Mayor Jack Ellis said he will assemble a committee to study

TBI's proposal and make a recommendation about whether to privatize. Meanwhile, TBI remains on a short−term contract expected to cost the city more than $80,000 from late February through the first week of April. Macon Chief Administrative Officer Regina McDuffie and other city officials have said that, with TBI's help, the airport should be able to comply with a Transportation Security Administration deadline Friday, March 31, to bring Middle Georgia Regional up to code.
Source: http://www.macon.com/mld/macon/14201409.htm

12. *March 28, Government Accountability Office* — **GAO−06−583T: Border Security: Investigators Transported Radioactive Sources Across Our Nation's Borders at Two Locations (Testimony).** Given today's unprecedented terrorism threat environment and the resulting widespread congressional and public interest in the security of our nation's borders, the Government Accountability Office (GAO) was asked to conduct an investigation testing whether radioactive sources could be smuggled across U.S. borders. Most travelers enter the United States through the nation's 154 land border ports of entry. Department of Homeland Security's U.S. Customs and Border Protection (CBP) inspectors at ports of entry are responsible for the primary inspection of travelers to determine their admissibility into the United States and to enforce laws related to preventing the entry of contraband, such as drugs and weapons of mass destruction. GAO's testimony provides the results of undercover tests made by its investigators to determine whether monitors at U.S. ports of entry detect radioactive sources in vehicles attempting to enter the United States. GAO also provides observations regarding the procedures that CBP inspectors followed during its investigation. GAO is also issuing a report on the results of this investigation.
Highlights: http://www.gao.gov/highlights/d06583thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−583T

13. *March 28, Government Accountability Office* — **GAO−06−562T: Federal Aviation Administration: An Analysis of the Financial Viability of the Airport and Airway Trust Fund (Testimony).** The Airport and Airway Trust Fund was established by the Airport and Airway Revenue Act of 1970 (P.L. 91−258) to help fund the development of a nationwide airport and airway system and to fund investments in air traffic control facilities. It provides all of the funding for the Federal Aviation Administration's (FAA) capital accounts, including: (1) the Airport Improvement Program, which provides grants for construction and safety projects at airports; (2) the Facilities and Equipment account, which funds technological improvements to the air traffic control system; and (3) the Research, Engineering, and Development account, which funds continued research on aviation safety, mobility, and environment issues. In addition, at various times during its history, the Trust Fund has funded all or some portion of FAA's operations. To fund these accounts, the Trust Fund is credited with revenues from a variety of excise taxes related to passenger tickets, passenger flight segments, international arrivals/departures, cargo waybills, and aviation fuels. Including interest earned on its balances, the Trust Fund received $10.8 billion in fiscal year 2005. The various taxes that accrue to the Trust Fund are scheduled to expire at the end of fiscal year 2007. The Government Accountability Office was asked to provide information and analysis about the financial condition and future viability of the Trust Fund.
Highlights: http://www.gao.gov/highlights/d06562thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−562T

14. *March 27, Defense News* — **U.S. Coast Guard changes Cutter building program.** Three of the most visible elements of the U.S. Coast Guard’s Deepwater modernization program are undergoing acquisition changes that will alter when the new ships are purchased and enter service, Deepwater officials said Monday, March 27. The Coast Guard no longer plans to interrupt the construction of its eight large National Security Cutters (NSC) midway through the program to begin construction of the medium−size Offshore Patrol Cutter (OPC). Rather, said Bob Conrad, vice president of operations for Integrated Coast Guard Systems (ICGS), an industry consortium that manages Deepwater for the Coast Guard, the service now will build one NSC per year through fiscal 2011, with construction of the first OPC to follow in 2012. Building all eight NSC cutters without interruption allows for better production efficiencies, Conrad said, and returns the first year of OPC acquisition to the original Deepwater plan approved in 2002. OPC construction had been moved up in response to several recommendations, including a RAND study that urged the ships be purchased sooner than planned.
Source: http://www.defensenews.com/story.php?F=1647081&C=america

15. *March 27, Transportation Security Administration* — **TSA establishes permanent screening operations at Manhattan Heliport.** The Transportation Security Administration (TSA) announced on Monday, March 27, that it has established a screening presence at the Downtown Manhattan Heliport at Wall Street. This operation represents the first time since TSA’s inception that it has assigned screening personnel and equipment to a heliport facility. Working with the heliport’s operator, the Port Authority of New York and New Jersey, TSA has enacted a Heliport Security Plan (HSP), which will ensure that the Wall Street facility adheres to all of TSA’s regulatory requirements and applicable Security Directives. Construction modifications at the heliport have created a “sterile area” that will physically separate screened individuals and their baggage from non−screened individuals. Having already satisfied TSA's passenger and baggage screening requirements at the heliport, U.S. Helicopter passengers and baggage departing the Downtown Manhattan Heliport will be able to connect to commercial flights within the sterile areas at JFK Airport. Future plans include additional commercial helicopter flights from the heliport to Newark Liberty International and LaGuardia Airports operating under the same sterile to sterile concept.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 01bf452

16. *March 27, Associated Press* — **Passengers rescued after cruise ship runs aground on Columbia.** The nearly 200 passengers aboard a luxury sternwheeler cruise ship made it to shore in good spirits Friday night, March 24, after the ship ran aground in the Columbia River. The 360−foot Empress of the North struck a sandbar Friday morning in the river channel near Washougal, WA. Passengers and crew remained onboard for more than eight hours until they were loaded, via a barge, to a sister sternwheeler. The recovery ship, the 230−foot Queen of the West, took passengers and crew to the nearby Port of Washougal. Passengers said when they hit the sandbar, the boat jolted and rumbled like it was riding over gravel. Guests said the staff quickly informed them that the ship was trying to avoid an upcoming barge and as a result, accidentally hit a sandbar. The Multnomah County Sheriff's office said wind and choppy waters may have sent the vessel off course. The Empress of the North ran aground in 2003 in the Columbia River near The Dalles. That grounding was blamed on human error, company officials said.
Source: http://www.usatoday.com/travel/news/2006−03−27−cruise−runs−a ground_x.htm

17. *March 22, Government Accountability Office* — **GAO−06−389: Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports−of−Entry, but Concerns Remain (Report).** Preventing radioactive material from being smuggled into the United States is a key national security objective. To help address this threat, in October 2002, DHS began deploying radiation detection equipment at U.S. ports−of−entry. This report reviews recent progress DHS has made (1) deploying radiation detection equipment, (2) using radiation detection equipment, (3) improving the capabilities and testing of this equipment, and (4) increasing cooperation between DHS and other federal agencies in conducting radiation detection programs. The Secretary of Homeland Security should work with other agencies, as necessary, to (1) streamline internal review procedures so that spending data can be provided to the Congress in a more timely way; (2) update the current deployment plan; (3) analyze the benefits and costs of advanced portals, then revise the program's cost estimates to reflect current decisions; (4) develop ways to effectively screen rail containers; (5) revise agency procedures for container inspection; and (6) develop a way for CBP officers to verify NRC licenses. In commenting on a draft of this report, DHS stated that it agreed with, and will implement, the Government Accountability Office's recommendations.
Highlights: http://www.gao.gov/highlights/d06389high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−389

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

Nothing to report.

[Return to top]

Food Sector

Nothing to report.

[Return to top]

Water Sector

18. *March 27, News & Observer (NC)* — **State failing to ensure suppliers test water.** A News & Observer investigation shows that the North Carolina agency responsible for making sure drinking water is safe isn't getting the job done. The Public Water Supply Section, with 98 employees, has been overwhelmed trying to monitor safety tests required of nearly 7,000 public water systems. Those tests include checks for contaminants such as arsenic. Systems must also test for bacteria that can sicken or kill, but thousands of small systems don't obey laws requiring them to test their water and clean up contamination. The state has been unable to force

compliance. North Carolina has more public water systems than any other Southern state and double the national average. Most are small operations serving a few dozen to a few hundred people in rural neighborhoods or supplying water to schools, churches, day−care centers or small businesses in out−of−the−way places. Thousands of them aren't performing required tests, records show.
Source: http://www.newsobserver.com/1171/story/422480.html

19. *March 27, Associated Press* — **Waikiki sewer main break spills one million gallons into canal.** More than one million gallons of raw sewage has been diverted into the Ala Wai Canal since the major sewer line break in Waikiki, HI, Friday, March 24. It was the largest of at least a half−dozen sewage spills on Oahu in the past few days caused by heavy rains.
Source: http://www.kpua.net/news.php?id=7832

[Return to top]

Public Health Sector

20. *March 28, Czech News Agency* — **Bird flu found in Czech Republic.** The swan found dead on the Vltava river near Hluboka nad Vltavou, south Bohemia, on Monday, March 27, probably died from the highly pathogenic virus H5N1, Agriculture Minister Jan Mladek told journalists after a meeting of the National Security Council Tuesday, March 28. The final word will be given by experts from a British lab.
Source: http://www.ctk.cz/english/services/english/index_view.php?id =180245

21. *March 28, Agence France−Presse* — **Indian officials to slaughter more chickens after new bird flu cases.** Indian officials were due Wednesday, March 28, to return to the scene of a bird flu outbreak to slaughter 250,000 more chickens after new confirmed cases in villages. Teams of animal health workers will expand a slaughter zone across 580 square miles after laboratory tests confirmed the outbreak was wider than first thought, said Bijay Kumar, commissioner of animal husbandry for the western state of Maharashtra. A total of 11 villages have been affected in two neighboring states in and around the district of Jalgaon since the outbreak was first confirmed two weeks ago. Officials have so far slaughtered 100,000 birds after four cases were confirmed in Jalgaon, 85 miles from the town of Navapur where India's first cases were reported in February.
Source: http://news.yahoo.com/s/afp/20060328/hl_afp/healthfluindia_0
60328144244;_ylt=Apo53GK0JgUDbqOg9jh3j5GJOrgF;_ylu=X3oDMTA5a
HJvMDdwBHNlYwN5bmNhdA−−

22. *March 27, Associated Press* — **Second Egyptian woman dies of bird flu.** A 30−year−old woman died of the H5N1 bird flu strain on Monday, March 27, Egypt's second human death from the virus since it appeared in the country last month, the health ministry announced. Fatma Mahmoud Youssef Sabra came from a village just north of Cairo, near Egypt's other human bird flu death, said Abdel−Rahman Shahin of the health ministry.
Source: http://abcnews.go.com/Health/wireStory?id=1773637

23.

March 23, Stanford School of Medicine — **Researchers find new approach to thwart anthrax toxicity.** Most methods of fighting microbial infection focus on killing the microbe, but the bacteria or virus is just one half of the equation. Researchers at the Stanford University School of Medicine found a method of finding human genes that, when inactivated, can also thwart infection. Using this technique, the group found a way to make cells resistant to the deadly anthrax toxin. Drugs that block proteins made by host genes could provide a new class of antimicrobial drugs, the researchers said. They could also be a much−needed second line of defense in cases where microbes develop resistance to antibiotics or antiviral agents. Researchers discovered that the LDL receptor−related protein known as LRP6 helps the toxin made by anthrax−producing bacteria enter a cell. The LRP6 protein in cells was inactivated in a laboratory dish using an antibody. These cells became resistant to the anthrax toxin.
Abstract: http://www.cell.com/content/article/abstract?uid=PIIS0092867 406001991
Source: http://mednews.stanford.edu/releases/2006/march/cohen.html

[Return to top]

Government Sector

24. *March 28, Government Accountability Office* — **GAO−06−462T: Homeland Security: Better Management Practices Could Enhance DHS's Ability to Allocate Investigative Resources (Testimony).** Immigration and Customs Enforcement's (ICE) mission is to prevent terrorist attacks within the United States and reduce the vulnerability of the United States to terrorism while ensuring its mandated customs, immigration, and federal protective enforcement functions are not diminished. The ICE Office of Investigations (OI) supports that mission by investigating customs and immigration violations. This testimony addresses the following key questions that were answered in GAO−06−48SU, a restricted report issued with the same title: (1) What structure and activities has OI adopted to address its mission? (2) In fiscal year 2004 and the first half of fiscal year 2005, how did OI use its investigative resources to achieve its goals? (3) How does OI ensure that its resource use contributes to its ability to prevent the exploitation of systemic vulnerabilities in customs and immigration systems? The Government Accountability Office (GAO) recommended that Homeland Security implement management practices to support resource allocation decisions, including a risk assessment, revised performance measures, and monitoring and communication systems to provide meaningful data about resource use. The Department of Homeland Security concurred with GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d06462thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−462T

[Return to top]

Emergency Services Sector

25. *March 27, Federal Computer Week* — **Alaska to test tsunami warning system.** Officials from the National Weather Service (NWS) and Alaska's emergency management office will test a tsunami communications warning system Wednesday, March 29. The test, which is being conducted in cooperation with local emergency management offices and the Alaska

Broadcasters Association, will broadcast live tsunami warning codes −− rather than a test code −− across TV and radio stations, but the text of the message will likely indicate it is a test.
Source: http://www.fcw.com/article92746−03−27−06−Web

[Return to top]

Information Technology and Telecommunications Sector

26. *March 27, FrSIRT* — **Symantec Veritas NetBackup multiple daemons remote buffer overflow vulnerabilities.** Multiple vulnerabilities have been identified in Veritas NetBackup Master, Media Servers and clients, which could be exploited by remote attackers to take complete control of an affected system. Analysis: The first issue is due to a buffer overflow error in the volume manager daemon (vmd.exe) that does not properly handle malformed data sent to port 13701/TCP, which could be exploited by remote attackers to execute arbitrary commands. The second flaw is due to a buffer overflow error in the NetBackup Database Manager service (bpdbm.exe) that does not properly handle malformed data sent to port 13721/TCP, which could be exploited by remote attackers to compromise a vulnerable system. The third vulnerability is due to a buffer overflow error in the VERITAS Network Daemon (vnetd) that does not properly handle specially crafted messages sent to port 13724/TCP, which could be exploited by attackers to execute arbitrary commands. See source advisory for a complete list of vulnerable products.
Solution: Apply security updates: http://seer.support.veritas.com/docs/281521.htm
Source: http://www.frsirt.com/english/advisories/2006/1124

27. *March 27, Secunia* — **Microsoft .NET Framework SDK ildasm buffer overflow.** A vulnerability has been discovered in Microsoft .NET Framework SDK, which can be exploited by malicious people to cause a denial−of−service and potentially compromise a user's system. Analysis: The vulnerability is caused due to a boundary error within ildasm when disassembling a DLL file. This can be exploited to cause a heap based buffer overflow when a specially crafted DLL is disassembled. Affected software: Microsoft .NET Framework 1.x.
Solution: Do not use ildasm to disassemble untrusted DLL files.
Source: http://secunia.com/advisories/19406/

28. *March 27, Security Focus* — **Microsoft Office XP array index denial−of−service vulnerability.** Microsoft Office is prone to a denial−of−service condition when handling malformed array indices. Analysis: When an Office application such as Excel, Word, or PowerPoint tries to open a file containing a malformed array index, an exception will be thrown, causing the application to fail. For a complete list of vulnerable products:
http://www.securityfocus.com/bid/17252/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/17252/references

29. *March 27, ZDNet (UK)* — **Microsoft creates public bug database for Internet Explorer.** Microsoft is for the first time encouraging people to give public feedback on Internet Explorer (IE), with the creation of a bug database for the next version of its browser, IE 7 beta. The bug database is accessible from the Microsoft Connect site and can be accessed by anyone that has a

Microsoft Passport account.
Source: http://news.zdnet.co.uk/software/applications/0,39020384,392 59531,00.htm

30. *March 27, Washington Technology* — **Council to draw up cyber attack response.** Setting up a national IT disaster response apparatus is one possible topic to be addressed by the IT Sector Coordinating Council as it drafts a sector−specific plan for protecting the nation's computer networks against a terrorist attack or other disaster, according to the group's chairman. The goal is for private sector IT companies and government to work together to prevent and to respond to cyber attacks. The council wants ideas from the IT industry and from the Department of Homeland Security as it begins work on the sector−specific critical infrastructure protection plan at its Tuesday, April 4, meeting. The council expects to complete the plan by September.
Source: http://www.washingtontechnology.com/news/1_1/homeland/28284− 1.html

31. *March 26, Netcraft* — **Domain registrar Joker under attack.** Domain registrar Joker.com says its name servers are under attack, causing outages for customers. More than 550,000 domains are registered with Joker, which is based in Germany. Any of those domains that use Joker's DNS servers are likely to be affected.
Source: http://news.netcraft.com/archives/2006/03/26/domain_registra
r_joker_hit_by_ddos.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a vulnerability in the way Microsoft Internet Explorer handles the createTextRange() DHTML method. By persuading a user to access a specially crafted webpage, a remote, unauthenticated attacker may be able to execute arbitrary code on that user's system. This vulnerability can also be used to crash Internet Explorer. We are aware of proof of concept code for this vulnerability. More information about the reported vulnerability can be found in the following US−CERT Vulnerability Note:

VU#876678 − Microsoft Internet Explorer createTextRange() vulnerability
http://www.kb.cert.org/vuls/id/876678

Known attack vectors for this vulnerability require Active Scripting to be enabled in Internet Explorer. Disabling Active Scripting will reduce the chances of exploitation. Until an update, patch or more information becomes available, US−CERT recommends disabling Active Scripting as specified in the Securing Your Web Browser document.
http://www.us−cert.gov/reading_room/securing_browser/#how_to _secure

We will continue to update current activity as more information becomes available.

TSP Phishing Scams

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. Specifically, sites that provide online benefits are being targeted. Recently, the phishing scam targeted the Thrift Savings Plan (TSP), a retirement savings plan for United States government employees and members of the uniformed services. For more information please see Thrift Savings Plan (TSP) at URL: http://www.tsp.gov/

If you were affected by the TSP phishing scam, please refer to the TSP E−mail scam instructions for assistance. http://www.tsp.gov/curinfo/emailscam.html

US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Additionally, users are encouraged to take the following measures to prevent phishing attacks from occurring:

Do not follow unsolicited web links received in email messages.

Contact your financial institution immediately if you believe your account and/or financial information has been compromised.

Current Port Attacks

Top 10 Target Ports	6346 (gnutella−svc), 1026 (win−rpc), 445 (microsoft−ds), 80 (www), 135 (epmap), 1025 (win−rpc), 139 (netbios−ssn), 1027 (icq), 1434 (ms−sql−m), 2745 (Bagle.C) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

32. *March 28, Honolulu Advertiser (HI)* — **Landowners take long, hard look at dams.**
Landowners across Hawaii are closely examining reservoirs and dams they own after the March 14 Kaloko Dam collapse that killed seven people living along the Wailapa Stream. For

example, A&B's Kauai Coffee Co. has drained its Aepo Reservoir in Lawai and other reservoirs it operates in the area. While it is standard practice for the company to lower water levels during heavy rains, it took an extra step in this situation. Some owners, including the state, are reviewing how much reservoir storage is actually needed, and some operators already have reduced the capacities maintained in reservoirs to reflect smaller demand. Several reservoirs across the state had already been shut down before the Kaloko disaster, generally because there were no longer agricultural uses for the water they stored. Joint state−federal dam inspection crews have completed studies of all of Kauai's reservoir dams, and plan to look at every dam in the state during the next four days.
Source: http://www.honoluluadvertiser.com/apps/pbcs.dll/article?AID=/20060328/NEWS01/603280359/1001/NEWS

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.